

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

PLAINTIFF,

v.

APPROXIMATELY 9.55075247 BITCOIN SEIZED
FROM BINANCE ACCOUNT ENDING 1454,
APPROXIMATELY 80.92772386 ETHER SEIZED
FROM BINANCE ACCOUNT ENDING 1454, AND
APPROXIMATELY 16341.9 POLYGON SEIZED
FROM BINANCE ACCOUNT ENDING 1454,

DEFENDANTS.

CIVIL ACTION No.:

VERIFIED COMPLAINT FOR FORFEITURE

NOW COMES Plaintiff United States of America, by Ryan K. Buchanan, United States Attorney, and Norman L. Barnett, Assistant United States Attorney, for the Northern District of Georgia, and shows the Court the following in support of its Verified Complaint for Forfeiture:

NATURE OF THE ACTION

1. This is a civil forfeiture action against digital currency seized from various accounts maintained at Binance, a cryptocurrency exchange, arising from an investment money laundering scheme.

THE DEFENDANTS IN REM

2. The defendant property consists of the following digital currency that the United States Secret Service (“USSS”) seized, pursuant to a Federal seizure warrant, on or about December 28, 2023:
 - a. Approximately 9.55075247 Bitcoin (BTC) seized from Binance account ending 1454 (“TARGET ACCOUNT”),
 - b. Approximately 80.92772386 Ether (ETH) seized from TARGET ACCOUNT, and
 - c. Approximately 16341.9 Polygon (MATIC) seized from TARGET ACCOUNT.(collectively, “Defendant Property”).

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1345 and 1355.
4. This Court has in rem jurisdiction over the Defendant Property pursuant to 28 U.S.C. § 1355(b)(1)(A) because acts or omissions giving rise to the forfeiture occurred in this district.
5. Venue is proper in this district pursuant to 28 U.S.C. § 1355(b)(1)(A) because the acts or omissions giving rise to the forfeiture occurred in this district.

6. The Defendant Property is presently being held in a custodial virtual wallet maintained by the United States Secret Service.

BASIS FOR FORFEITURE

Relevant Statutes

7. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) on the grounds that it constitutes or was derived from proceeds traceable to a violation of 18 U.S.C. § 1349 (conspiracy to commit wire fraud).
8. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C) on the grounds that it constitutes or was derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud).
9. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) on the grounds that it constitutes property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956 (money laundering), or is property traceable to such property.
10. The Defendant Property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) on the grounds that it constitutes property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1957 (money laundering), or is property traceable to such property.

Factual Background

11. An investigation by the USSS revealed the following:

Relevant Definitions

12. “Pig butchering” is a type of romance scam wherein the perpetrators pretend to engage in a romantic relationship with a victim – that is exclusively virtual – for the sole purpose of defrauding the victim out of money.
13. The victims in pig butchering schemes are referred to as “pigs” by the co-conspirators because the co-conspirators use elaborate romantic storylines to “fatten up” victims into believing they are in a romantic relationship.
14. The co-conspirators then introduce to the victim a purported investment cryptocurrency opportunity.
15. Specifically, the co-conspirators claim that they have been investing in cryptocurrency and experiencing drastic profitable returns. The co-conspirators defraud the victims into believing that they also can experience the profitable returns by investing in the same cryptocurrencies. As part of the scheme, the co-conspirators will direct the victims to fake websites or applications that are designed to look like cryptocurrency investment platforms. In reality, the websites or applications have limited functionality

and do not provide the user any access to a cryptocurrency platform or cryptocurrency wallet.

16. The co-conspirators also may show victims images of fake cryptocurrency transactions to further create the impression that the co-conspirators are contributing their own funds to the purported cryptocurrency investment opportunity.
17. The co-conspirators then refer to “butchering” or “slaughtering” the victims once the victim transfers the assets to the fake cryptocurrency investment platform, which actually are transferred to wallets that the co-conspirators control.
18. “Virtual currencies” or cryptocurrencies are digital assets designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. Cryptocurrencies are circulated over the Internet as a form of value. Cryptocurrencies operate independently of a central bank. Cryptocurrencies are similar to paper currency in that the exchange of cryptocurrencies between individuals is not recorded by financial institutions. Cryptocurrencies are not issued by any government, bank or company, but rather are generated and controlled through computer

software operating via a decentralized peer-to-peer network.

19. The “blockchain” is essentially a distributed public ledger, run by a decentralized network, containing an immutable and historical record of every transaction utilizing that blockchain’s technology. It can be updated multiple times per hour and records every virtual currency address that ever received that virtual currency. The blockchain also maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.
20. Cryptocurrencies are sent to and received from “addresses.” An address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or PIN needed to access the address. Only the holder of an address’s private key can authorize any transfers of cryptocurrencies from that address to other addresses.
21. To transfer a cryptocurrency to another address, the payor transmits a transaction announcement, cryptographically signed with the payor's private key, across the network. The address of the receiving party and the

sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the payor or payee is transmitted in a transaction itself. Once the payor's transaction announcement is verified, the transaction is added to the blockchain. The blockchain logs every address that has ever received a cryptocurrency and maintains records of every transaction for each address.

22. "Cryptocurrency exchanges" are businesses that allow customers to trade cryptocurrencies for other assets, such as conventional fiat money or other virtual currencies.
23. "Binance" is a cryptocurrency exchange and custodian that allows customers to buy, sell, and store virtual assets. Binance Global, the Binance entity relevant to this complaint, is incorporated in the Cayman Islands.
24. Due to the encrypted nature of cryptocurrency and the anonymous nature of cryptocurrency transactions, the identity of a Binance account's owner is untraceable, unless the owner decides to make such information publicly available.
25. "crypto.com" is a legitimate cryptocurrency exchange in which users can purchase, send, receive, and trade virtual currencies.

26. “Coinbase” is a legitimate online platform for buying, selling, transferring, and storing cryptocurrency.
27. The “Coinbase Wallet” application is a legitimate cryptocurrency wallet application for smartphones that provides users with a non-custodial cryptocurrency wallet. The Coinbase Wallet application also includes a web browser that enables users to access websites that allow them to connect their wallet to decentralized applications.
28. “Non-custodial wallets” allow users to send and receive virtual currencies without being tied to the Coinbase exchange itself.
29. A “decentralized application,” or “dApp,” is a software program or digital application that operates on a blockchain or peer-to-peer network rather than a single computer. Decentralized applications are used for several purposes, including wallets and exchanges, and are often developed to operate on the Ethereum blockchain.
30. “Ethereum” is an open source, public blockchain-based distributed computing platform and operating system that hosts USDT, ETH, BTC, MATIC, and other virtual currencies.
31. “Bitcoin,” widely known as “BTC,” is a blockchain-based cryptocurrency that allows users to conduct transactions on decentralized networks

independently of a centralized bank and/or fiat currency.

32. “Tether,” widely known as “USDT,” is a blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. Dollars, making it what is known as a “stablecoin.”
33. USD Coin, widely known as “USDC,” is another blockchain-based cryptocurrency whose tokens in circulation are backed by an equivalent amount of U.S. Dollars. It is also a stablecoin.
34. “Ether,” widely known as “ETH” is a cryptocurrency that is open source, public, has a blockchain, and is distributed on a platform. The public ledger is the digital trail of the Ethereum blockchain, which allows anyone to track the movement of ETH.
35. A “transaction hash” is a unique string of letters and numbers generated when a cryptocurrency transaction is initiated. Records of transaction hashes are permanent and publicly available on the Ethereum blockchain.
36. A “wallet” is a software application that interfaces with the virtual currency’s specific blockchain and generates and stores a user’s addresses and private keys. A virtual currency wallet also allows users to send and receive virtual currencies. Multiple addresses can be stored in a wallet.

The Pig Butchering Scheme Targeting Victims AD and DD

37. In or around May 2022, the USSS began investigating a suspected pig butchering scheme after it received a complaint from an individual with the initials DD.
38. DD reported that DD, DD's sibling, who is an individual with the initials AD, and other family members were victims of a cryptocurrency investment scam.
39. DD and AD resided in the Northern District of Georgia during all times relevant to this Complaint.
40. DD reported that, in or around October 10, 2022, AD connected with an individual identifying herself as "Junia" via an SMS text message.
41. Junia told AD that she messaged AD by mistake while looking for someone else. Despite the fact that the message supposedly was sent to the wrong person, AD and Junia continued to communicate via text message.
42. Eventually, Junia began discussing a business she purportedly owned and sent AD a web address linked to her purported business.
43. Junia told AD that Junia invested and traded in cryptocurrency using an Ethereum Coinbase wallet through the Coinbase application linked to a separate supposed application only available through a website called web-

hft.com.

44. Based on Junia's instructions, AD opened an account on crypto.com in order to trade and invest in cryptocurrency and also downloaded the Coinbase Wallet application to create a wallet to hold her cryptocurrency.
45. Per Junia's instruction, AD also linked AD's Coinbase wallet to a separate application purportedly hosted by web-hft.com.
46. Also, at Junia's instruction, AD purchased USDT from crypto.com and transferred USDT to AD's Coinbase wallet, which gave the appearance that AD was in control of AD's funds following the transfer of USDT to AD's Coinbase wallet.
47. When AD viewed AD's account on web-hft.com, it appeared that AD's investments were profitable.
48. Learning about AD's profitable investments, DD began to provide funds to AD to deposit into AD's Coinbase wallet in order to invest in cryptocurrency through web-fht.com.
49. Between approximately September 2022 and November 2022, AD and DD transferred more than 269,000 USDT to AD's Coinbase wallet.
50. In or around October 2022, AD and DD were attempting to complete an investment order through web-hft.com using funds in AD's Coinbase wallet

and discovered that the funds in AD's Coinbase wallet were no longer accessible.

51. AD and DD contacted web-hft.com via the information provided in the application.
52. A supposed customer support agent at web-hft.com known as "G" told AD that the web-hft.com account was currently locked due to penalties on the account based on supposed damage to the operating system for not completing an order for an extended period of time.
53. G also told AD that, to unlock the account, AD must pay a 30% fee – more than the equivalent of approximately \$115,000.00(USD). G further threatened AD that if the fee was not paid, web-hft.com would take legal action and report AD to the FBI.
54. DD and AD asked if they could use money from their web-hft.com account to pay the fee, but G said that the fee had to be paid using outside funds and suggested that AD take out a loan to pay the fee.
55. The investigation revealed that web-hft.com is not a cryptocurrency trading platform at all and, instead, appears to be a website designed for the sole purpose of defrauding individuals into believing that they are using a cryptocurrency trading platform.

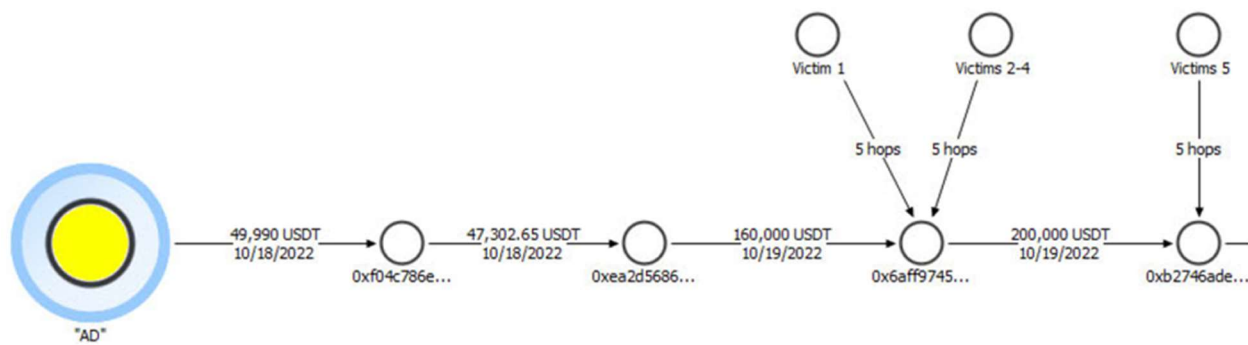
56. The investigation further revealed that there was no legitimate connection between web-hft.com and the Coinbase wallet application and that the perpetrators actually gained access to AD's Coinbase wallet when AD was led to believe that AD was linking AD's Coinbase wallet to a supposed account on the fake web-hft.com.

Fraud Proceeds Obtained from AD were Transferred to TARGET ACCOUNT

57. USSS's review of the Ethereum blockchain verifies the transactions made by AD and further reflects that AD's funds were transferred to the TARGET ACCOUNT and other addresses that received other known fraud proceeds.
58. Specifically, the Ethereum blockchain reflects that, between October 19, 2022, and January 6, 2023, AD's funds were laundered through a total of approximately 20 hops on the Ethereum blockchain before arriving at the TARGET ACCOUNT.
59. On or about October 18, 2022, AD sent 49,990.00 USDT from AD's Coinbase wallet to an Ethereum blockchain address beginning with 0xf04c786e as part of the web-hft.com investment scheme.
60. That same day, 47,302.65 USDT was sent to an Ethereum blockchain address beginning with 0xea2d5686.
61. The following day, on October 19, 2022, AD's funds were commingled with

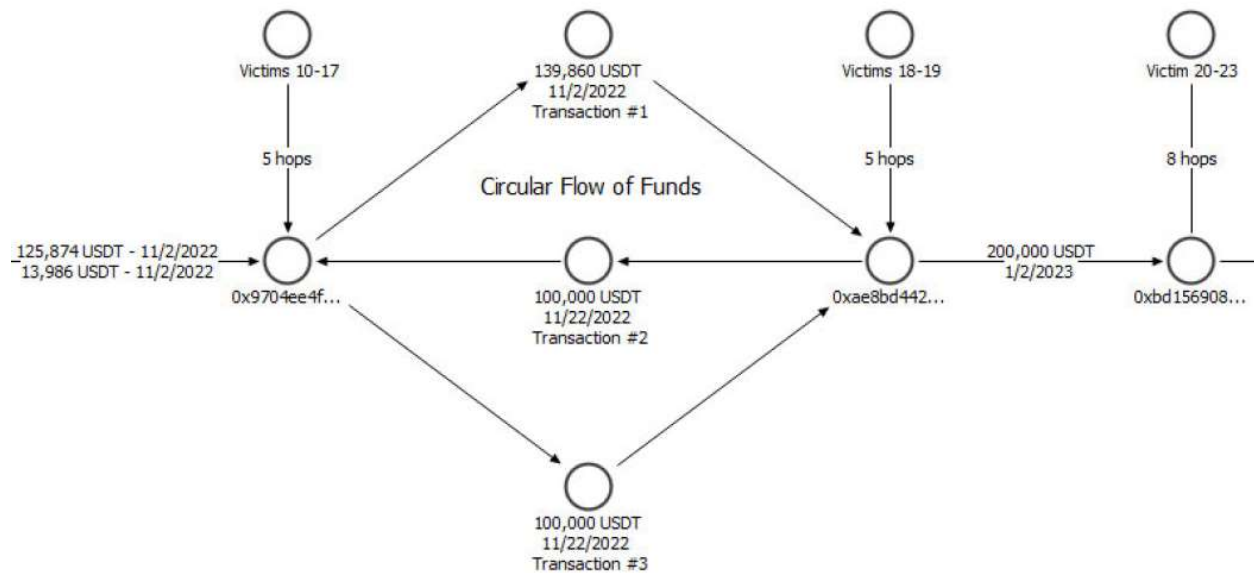
additional USDT in the Ethereum blockchain address beginning with 0x6aff9745 before AD's funds, along with other victim funds, were transferred to the Ethereum blockchain address beginning with 0xb2746ade.

62. The following diagram illustrates the transactions described above in Paragraphs 57 through 61.



63. USSS determined that, on or about November 2, 2022, AD's funds, after being commingled with other victims' funds, were transferred through several hops that formed a circular flow of funds.
64. For example, in November 2022, AD's funds, which were commingled with other victims' funds, were sent from the Ethereum blockchain address beginning 0x9704ee4f to the address beginning 0xae8bd442. The funds were then sent back the address beginning 0x9704ee4f before being returned to the address beginning 0xae8bd442 and hopped to an address beginning 0xbd156908 on or about January 2, 2023.

65. The following diagram illustrates the circular flow of funds involving AD's funds and other victim funds before they were transferred into the TARGET ACCOUNT.



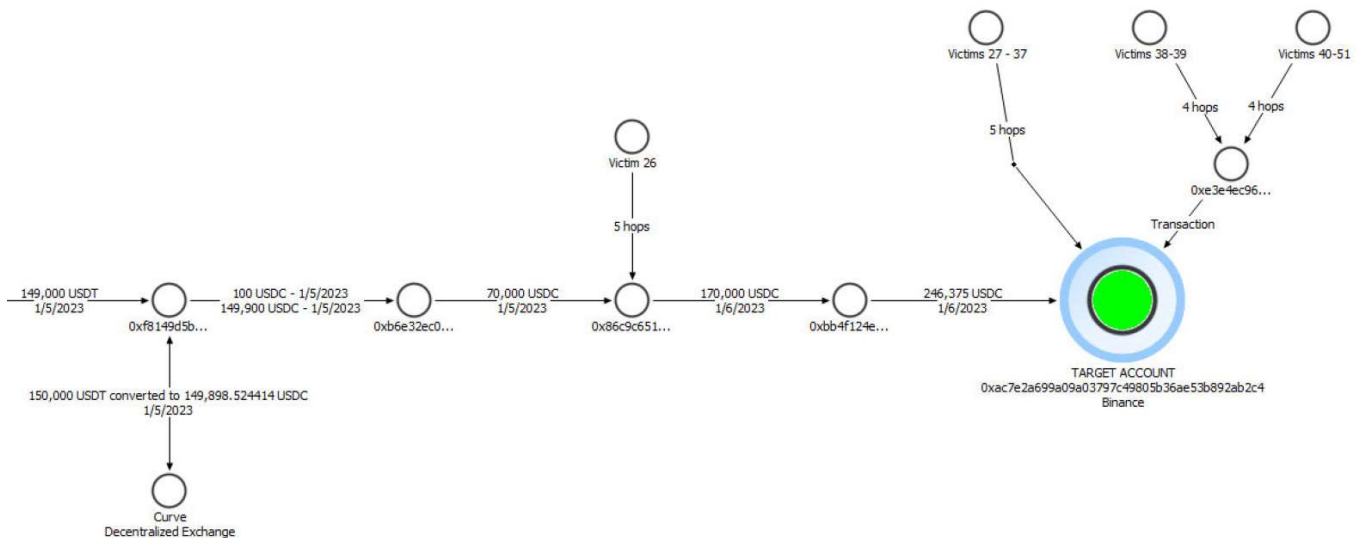
66. There is no apparent lawful purpose for funds to move in a circular pattern, as there are transaction fees known as "gas" associated with each transfer on the Ethereum blockchain. The additional unnecessary expense of moving money in such a manner is likely an attempt to further evade law enforcement and is consistent with money laundering activity.
67. Moreover, money launderers often conduct an otherwise unnecessary number of transactions in the transfer of funds in an effort to layer ill-gotten

funds to ultimately conceal or disguise the nature, location, source, ownership, or control of those proceeds when they are ultimately transferred into a cryptocurrency exchange. The number of hops in this transaction is a strong indication that the movement of funds was performed in a manner meant to conceal or disguise the nature, location, source, ownership, or control of the proceeds of a specified unlawful activity, to wit, wire fraud.

68. During the series of hops transferring AD's funds to the TARGET ACCOUNT, AD's funds were converted from USDT to USDC.
69. Specifically, the Ethereum blockchain reflects that, on January 5, 2023, AD's funds, which were commingled with USDT from other victims, were transferred into the Ethereum blockchain address beginning 0xf8149d5b.
70. The funds were then transferred into Curve, a decentralized cryptocurrency exchange, and converted into USDC before being hopped to subsequent addresses on the Ethereum blockchain.
71. Converting funds to different types of cryptocurrencies is another indication of layering transactions to evade law enforcement authorities by attempting to conceal the source of proceeds.
72. The next day, on January 6, 2023, AD's funds and other victim funds were

transferred into the TARGET ACCOUNT.

73. The following diagram illustrates the transactions described above in Paragraphs 69 through 72.



74. USSS reviewed records for three accounts held at cryptocurrency exchanges, including the TARGET ACCOUNT, that received AD's funds, and determined that the accounts were consistent with pig butchering schemes because the accounts displayed a history of frequent, large dollar deposit transactions followed by a pattern of rapid movement of funds with large corresponding withdrawals.

The TARGET ACCOUNT is Associated with Fraud Schemes Targeting Other Victims

75. USSS determined that other victims who reported being victimized through

fraudulent investment schemes were associated with Ethereum blockchain addresses connected with the TARGET ACCOUNT.

76. More specifically, USSS analyzed the addresses used in hops between victim AD sending USDT to web-hft and AD's funds reaching the TARGET ACCOUNT.
77. The analysis revealed that victims filed complaints with the Federal Bureau of Investigation's Internet Crime Complaint Center ("IC3") or the Federal Trade Commission's ("FTC's") Consumer Sentinel Database regarding the same Ethereum blockchain addresses through which AD's funds flowed before reaching the TARGET ACCOUNT.
78. The victims associated with the blockchain addresses connected to the TARGET ACCOUNT collectively reported losses totaling the equivalent of approximately \$6,357,064.09(USD).
79. Altogether, the TARGET ACCOUNT processed virtual currency equaling the equivalent of approximately \$248 million(USD) between 2020 and January 2023.

FIRST CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(C)

80. The United States re-alleges and incorporates by reference Paragraphs 1

through 79 of this Complaint as if fully set forth herein.

81. Based on the foregoing, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) on the grounds that the funds constitute or were derived from proceeds traceable to a violation of 18 U.S.C. § 1349 (conspiracy to commit wire fraud).

SECOND CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(C)

82. The United States re-alleges and incorporates by reference Paragraphs 1 through 79 of this Complaint as if fully set forth herein.
83. Based on the foregoing, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) on the grounds that the funds constitute or were derived from proceeds traceable to a violation of 18 U.S.C. § 1343 (wire fraud).

THIRD CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(A)

84. The United States re-alleges and incorporates by reference Paragraphs 1 through 79 of this Complaint as if fully set forth herein.
85. The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) on the grounds that the funds constitute property, real or personal, involved in a transaction or attempted transaction in

violation of 18 U.S.C. § 1956 (money laundering), or is property traceable to such property.

FOURTH CLAIM FOR FORFEITURE
18 U.S.C. § 981(a)(1)(A)

86. The United States re-alleges and incorporates by reference Paragraphs 1 through 79 of this Complaint as if fully set forth herein.
87. The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. §§ 981(a)(1)(A) on the grounds that the funds constitute property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1957 (money laundering), or is property traceable to such property.

/

/

/

/

/

/

/

PRAYER FOR RELIEF

WHEREFORE, the United States prays:

- (1) that the Court forfeit the Defendant Property to the United States of America;
- (2) that the Court award the United States the costs of this action; and
- (3) such other and further relief as the Court deems just and proper.

This 26th day of August 2024.

Respectfully submitted,

RYAN K. BUCHANAN

United States Attorney

75 Ted Turner Drive SW

Atlanta, GA 30303

(404) 581-6000 fax (404) 581-6181

/s/NORMAN L. BARNETT

Assistant United States Attorney

Georgia Bar No. 153292

Norman.barnett@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

PLAINTIFF,

v.

APPROXIMATELY 9.55075247 BITCOIN SEIZED
FROM BINANCE ACCOUNT ENDING 1454,
APPROXIMATELY 80.92772386 ETHER SEIZED
FROM BINANCE ACCOUNT ENDING 1454, AND
APPROXIMATELY 16341.9 POLYGON SEIZED
FROM BINANCE ACCOUNT ENDING 1454,

DEFENDANTS.

Civil Action No.

VERIFICATION OF COMPLAINT FOR FORFEITURE

I, Joshua Goetze, have read the Complaint for Forfeiture in this action and state that its contents are true and correct to the best of my knowledge and belief based upon my personal knowledge of the case and upon information obtained from other law enforcement personnel.

/

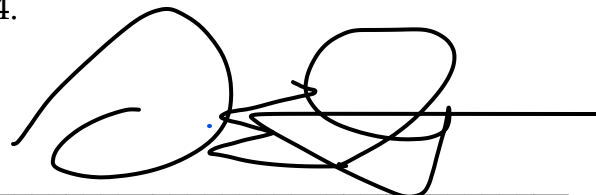
/

/

/

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

This 26th day of August 2024.

A handwritten signature in black ink, consisting of a large, stylized 'J' followed by a series of loops and a horizontal line extending to the right.

JOSHUA GOETZE
SPECIAL AGENT
UNITED STATES SECRET SERVICE